What is claimed is:

1. A method of recording digital data, comprising:

receiving packets of a digital data stream in a recording and playback device;

encrypting the packets in the recording and playback device according to an encryption key unique to the recording and playback device; and

storing the encrypted packets.

2. The method of claim 1, further comprising:

retrieving the encrypted packets;

decrypting the encrypted packets in the recording and playback device according to the encryption key unique to the recording and playback device; and

passing the decrypted packets to a presentation device;

whereby a copy of the encrypted packets will not play back intelligibly using other recording and playback devices,

whereby the encrypted packets are protected against unauthorized distribution.

3. The method of claim 1, wherein:

a first portion of said encryption key unique to a recording and playback device is hard-wired in said recording and playback device;

a second portion of said encryption key unique to said recording and playback device is stored in a memory associated with said recording and playback device;

said encryption key is formed in said recording and playback device according to a predetermined algorithm from said first portion and said second portion.

4. The method of claim 1, wherein:

a first portion of said encryption key unique to a recording and playback device is hard-wired in said recording and playback device;

a plurality of second portions of said encryption key unique to said recording and playback device are stored in a memory associated with said recording and playback device;

said encryption key is formed in said recording and playback device according to a predetermined algorithm from said first portion and one certain second portion from said plurality of second portions.

5. The method of claim 1, wherein:

a first portion of said encryption key unique to a recording and playback device is hard-wired in said recording and playback device;

a second portion of said encryption key unique to said recording and playback device is stored in a memory associated with said recording and playback device;

a third portion of said encryption key is entered by a user of the recording and playback device; and

said encryption key unique to said recording device is formed in said recording and playback device according to a predetermined algorithm from said first portion, said second portion, and said third portion,

whereby another user of said recording and playback device who does not know said third portion is precluded from obtaining intelligible playback of a recorded data stream.

6. The method of claim 1, wherein:

a packet comprises a first predetermined number of header bytes and a second predetermined number of payload bytes;

the header bytes are stored unencrypted; and

the payload bytes are stored encrypted,

whereby operations performable on the data stream that require access to header bytes but not to payload bytes are performable on the recorded data stream.

7. The method of claim 6, wherein stored packets are retrieved, header bytes are not decrypted, and payload bytes are decrypted..

8. The method of claim 6, wherein stored packets are retrieved, header bytes are replaced, and payload bytes are decrypted.

9. The method of claim 8, wherein:

the recording and playback device includes a random-access memory having a plurality of byte locations each corresponding to a different one of a plurality of first memory addresses;

bytes constituting a packet of the decrypted data stream appear sequentially at the output of a FIFO memory;

the output of the FIFO memory is mapped to a number of second memory addresses at least equal to the number of bytes comprising a packet;

the second memory addresses are contiguous with the first memory addresses;

the replacement header bytes are loaded into the n highest locations of the random-access memory, where n is the first predetermined number;

readout of the packet is accomplished by reading a number of the memory addresses equal to the sum of the first and second predetermined numbers commencing from the random-access memory address where the replacement header bytes commence.

10. The method of claim 2, further comprising: arranging a readout path for at least a portion of the encryption key to be disabled by a first irrevocable condition and to be re-enabled by a second irrevocable condition, and

arranging a path essential to functioning of the recording and playback device to be disabled by said second irrevocable condition.

11. The method of claim 10, comprising providing in the recording and playback device a one-time-programmable ROM, and wherein said first irrevocable condition comprises programming ON a first certain bit of the one-time programmable ROM, and wherein said second irrevocable condition comprises programming ON a second certain bit of the one-time programmable ROM.

12. The method of claim 11, further comprising storing said key portion bits in the one-time programmable ROM.

13. Apparatus for recording and playing back digital data, comprising:

a data receiver for receiving packets of a digital data stream;

an encrypter for encrypting the packets according to an encryption key unique to the apparatus; and

a data store for storing the encrypted packets.

14. The apparatus of claim 13, further comprising:

a decrypter for retrieving and decrypting the encrypted packets according to the encryption key unique to the apparatus; and

a data transmitter for passing the decrypted packets to a presentation device;

whereby a copy of the encrypted packets will not play back intelligibly using a different apparatus,

whereby the encrypted packets are protected against unauthorized distribution.

15. The apparatus of claim 13, further comprising:

permanent storage for storing a first portion of said encryption key unique to the apparatus;

a memory for storing a second portion of said encryption key unique to said apparatus;

key logic for forming said encryption key according to a predetermined algorithm from said first portion and said second portion.

16. The apparatus of claim 13, further comprising:

permanent storage for storing a first portion of said encryption key unique to the apparatus;

a memory for storing a plurality of second portions of said encryption key unique to said apparatus;

key logic for forming said encryption key to a predetermined algorithm from said first portion and one certain second portion from said plurality of second portions.

17. The apparatus of claim 13, further comprising:

permanent storage for storing a first portion of said encryption key unique to the apparatus;

a memory for storing a second portion of said encryption key unique to said apparatus;

a user interface for receiving a third portion of said encryption key; and

key logic for forming said encryption key unique to said recording device according to a predetermined algorithm from said first portion, said second portion, and said third portion,

whereby another user of said apparatus who does not know said third portion is precluded from obtaining intelligible playback of a recorded data stream.

18. The apparatus of claim 13, wherein:

a packet comprises a first predetermined number of header bytes and a second predetermined number of payload bytes;

the data store stores the header bytes unencrypted; and

the data store stores the payload bytes encrypted,

whereby operations performable on the data stream that require access to header bytes but not to payload bytes are performable on the recorded data stream.

19. The apparatus of claim 18, wherein stored packets are retrieved from the data store, header bytes are not decrypted, and payload bytes are decrypted by the decrypter.

20. The apparatus of claim 18, wherein stored packets are retrieved from the data store, control logic replaces header bytes, and payload bytes are decrypted.

21. The apparatus of claim 20, further comprising:

a random-access memory having a plurality of byte locations each corresponding to a different one of a plurality of first memory addresses;

a FIFO memory sequentially outputting bytes constituting a packet of the decrypted data stream, wherein:

the output of the FIFO memory is mapped to a number of second memory addresses at least equal to the number of bytes comprising a packet; and

the second memory addresses are contiguous with the first memory addresses, and wherein:

the control logic loads replacement header bytes into the n highest locations of the random-access memory, where n is the first predetermined number; and

the control logic reads out the packet by reading a number of the memory addresses equal to the sum of the first and second predetermined numbers commencing from the random-access memory address where the replacement header bytes commence.

22. The apparatus of claim 14, comprising a readout path for retrieving at least a portion of the encryption key and arranged to be disabled by a first irrevocable condition and to be re-enabled by a second irrevocable condition, and wherein recording and playback functioning of the apparatus is disabled by said second irrevocable condition.

23. The apparatus of claim 22, comprising a one-time-programmable ROM, and wherein said first irrevocable condition comprises programming ON a first certain bit of the one-time programmable ROM, and wherein said second irrevocable condition comprises programming ON a second certain bit of the one-time programmable ROM.

24. The method of claim 23, wherein said key portion is stored as bits in the one-time programmable ROM.

25. A recorder for recording digital data streams, encrypted according to a binary key at least a portion of which is stored in hardware of the recorder, comprising:

a readout path for retrieving said key portion, arranged to be disabled by a first irrevocable condition and re-enabled by a second irrevocable condition; and

at least one feature essential for recording and playback functioning of the recorder arranged to be disabled by said second irrevocable condition.

26. The recorder of claim 25, comprising a one-time-programmable ROM, and wherein said first irrevocable condition comprises programming ON a first certain bit of the one-time programmable ROM, and wherein said second irrevocable condition comprises programming ON a second certain bit of the one-time programmable ROM.

27. The recorder of claim 26, wherein said key portion comprises bits stored in the one-time programmable ROM.

28. A method practiced in a recorder for recording digital data streams, encrypted according to a binary key at least a portion of which is stored in hardware of the recorder, the recorder including a readout path for retrieving said key portion, the method comprising:

arranging said readout path to be disabled by a first irrevocable condition and re-enabled by a second irrevocable condition; and

arranging at least one feature essential for recording and playback functioning of the recorder to be disabled by said second irrevocable condition.

29. The method of claim 28, comprising providing in the recorder a one-time-programmable ROM, and wherein said first irrevocable condition comprises programming ON a first certain bit of the one-time programmable ROM, and wherein said second irrevocable condition comprises programming ON a second certain bit of the one-time programmable ROM.

30. The method of claim 29 further comprising storing said key portion bits in the one-time programmable ROM.

31. A set-top box for recording and playing back digital data, consisting of a housing which comprises:

a data receiver for receiving packets of a digital data stream;

an encrypter for encrypting the packets according to an encryption key unique to the set-top box; and

a data store for storing the encrypted packets.

32. The set-top box of claim 31, wherein the housing further comprises:

a decrypter for retrieving and decrypting the encrypted packets according to the encryption key unique to the set-top box; and

a data transmitter for passing the decrypted packets to a presentation device;

whereby a copy of the encrypted packets will not play back intelligibly using another set-top box,

whereby the encrypted packets are protected against unauthorized distribution.

33. The set-top box of claim 31, wherein the housing further comprises:

permanent storage for storing a first portion of said encryption key unique to the set-top box;

a memory for storing a second portion of said encryption key unique to said set-top box;

key logic for forming said encryption key according to a predetermined algorithm from said first portion and said second portion.

34. The set-top box of claim 31, wherein the housing further comprises:

permanent storage for storing a first portion of said encryption key unique to the set-top box;

a memory device for storing a plurality of second portions of said encryption key unique to said set-top box;

key logic for forming said encryption key to a predetermined algorithm from said first portion and one certain second portion from said plurality of second portions.